СХЕМЫ ВЫЧИСЛЕНИЯ СЕКРЕТА СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ДИНАМИЧЕСКИ ИЗМЕНЯЕМОЙ ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ

Калмыков И.А., Макарова А.В., Науменко Д.О., Березкина М.В.,
Северо-Кавказский федеральный университет,
Институт информационных технологий и телекоммуникаций,
г. Ставрополь, Россия,
alyonchikMav@yandex.ru

В настоящее время вопрос о защите информации стоит очень остро. В данной статье рассмотрены системы криптографической защиты информации, функционирующей в ПСКВ. Применение полиномиальной системы классов вычетов (ПСКВ) позволяет разрабатывать криптографические процедуры защиты информации, обеспечивающие в реальный масштаб времени закрытия информации. Использование в ПСКВ операций, связанных со сложением, умножением существенно улучшает обеспечение конфиденциальности и целостности информации.

Рассматривая схемы вычисления секрета систем криптографической защиты информации, функционирующей в полиномиальной системе классов вычетов, необходимо обеспечить безопасные связи внутри групп абонентов с динамически изменяющейся группой пользователей является актуальной задачей. Для предотвращения несанкционированного доступа постороннего пользователя, необходимо вычисление общего секретного ключа, который может быть определен только участниками группы. Каждому пользователю группы необходимо участвовать в генерации секретного ключа.

Существует несколько алгоритмов разделения секретного ключа на секретные доли.

Каждый из них предполагают, что ни один абонент группы не сможет вычислить пароль без помощи других абонентов группы. При этом любая схема разделения секрета состоит из двух взаимосвязанных протоколов: протокола формирования и распределения долей секрета между абонентами и протокола восстановления секрета группой пользователей с помощью их секретных долей. Первый протокол описывает последовательность действий системы и пользователей, в результате которых каждый авторизованный абонент получает свою долю секретного ключа. Второй протокол предназначен для того, чтобы законные пользователи, собравшись вместе и объединив свои секретные доли, могли восстановить секретный ключ.

В данной работе рассматриваются пороговая схема разделения секрета Шамира, пороговая схема разделения секрета Асмута–Блума, пороговая схема (m,n) разделения секрета с использованием полиномиальной системы классов вычетов.

Схема интерполяционных полиномов Лагранжа, схема разделения секрета Шамира или просто схема Шамира – это схема разделения секрета, широко используемая на практике. Схема Шамира позволяет создать (t, n)–пороговое разделение секрета для любых t, n. [1, 2]

Для построения схемы достаточно двух точек для задания прямой, трех точек – для задания параболы, четырех точек – для кубической параболы. Чтобы задать многочлен степени требуется точек.

Для того чтобы разделить секрет таким образом, чтобы восстановить его могли только k человек, его «прячут» его в формулу (k–1)–мерного многочлена. Восстановить этот многочлен можно по k точкам.

Пусть нужно разделить секрет M между n сторонами таким образом, чтобы любые k участников могли бы восстановить секрет (то есть нужно реализовать (k,n)–пороговую схему).

Выбираем некоторое простое число $p>M$. Это число можно открыто сказать всем участникам. Оно задаёт конечное поле размера P. Над этим полем построим многочлен степени $k–1$ (то есть случайно выбираются все коэффициенты многочлена, кроме M):

$$F(x) = (a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + M) \bmod P \qquad (1)$$

В этом многочлене M – это разделяемый секрет, а остальные коэффициенты $a_{k-1}, a_{k-2}, ..., a_1$ – некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

Теперь вычисляем координаты различных n точек:

$$\begin{aligned} k_1 &= F(1) = (a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + ... + a_1 \cdot 1 + M) \bmod p \\ k_2 &= F(2) = (a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + ... + a_1 \cdot 2 + M) \bmod p \\ &\cdots \\ k_i &= F(i) = (a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + ... + a_1 \cdot i + M) \bmod p \\ &\cdots \\ k_n &= F(n) = (a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + ... + a_1 \cdot n + M) \bmod p \end{aligned} \qquad (2)$$

Аргументы (номера секретов) не обязательно должны идти по порядку, главное – чтобы все они были различны по модулю P.

После этого секреты (вместе с их номером, числом P и степенью многочлена $k–1$) раздаются сторонам. Случайные коэффициенты $a_{k-1}, a_{k-2}, ..., a_1$ и сам секрет M «забываются».

Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них – разделённый секрет.

Особенностью схемы является то, что даже $k–1$ сторон, собравшихся вместе, не смогут найти секрет даже методом полного перебора всех возможных вариантов.

Прямолинейное восстановление коэффициентов многочлена через решение системы уравнений можно заменить на вычисление интерполяционного многочлена Лагранжа. Формула многочлена будет выглядеть следующим образом:

$$F(x) = \sum_i l_i(x) y_i \bmod p \qquad (3)$$

$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \bmod p$$

где (x_i, y_i) – координаты точек многочлена. Все операции выполняются также в конечном поле *P*.

Схема Асмута-Блума – пороговая схема разделения секрета, построенная с использованием простых чисел. Позволяет разделить секрет между n сторонами таким образом, что его смогут восстановить любые *m* участников. [1, 3]

Пусть *M* – некоторый секрет, который требуется разделить. Выбирается простое число *p*, большее *M*. Выбирается *n* взаимно простых друг с другом чисел $d_1, d_2, ..., d_n$, таких что:

$$\begin{gathered} \forall i : d_i > p \\ \forall i : d_i < d_{i+1} \\ d_1 * d_2 * ... d_m > p * d_{n-m+2} * d_{n-m+3} * ... * d_n \end{gathered} \quad (4)$$

Выбирается случайное число *r* и вычисляется

$$M' = M + rp \quad (5)$$

Вычисляются доли:

$$k_i = M' \bmod d_i \quad (6)$$

Участникам раздаются $\{p, d_i, k_i\}$

Теперь, используя китайскую теорему об остатках можно восстановить секрет *M* имея *m* и более долей.

Повысить эффективность работы схемы Асмута-Блума можно за счет перехода к ПСКВ.

Рассмотрим пороговую схему (*m*,*n*) разделения секрета с использованием полиномиальной системы классов вычетов.

В данной схеме используются неприводимые полиномы $p_i(z)$. Для реализации (*m*,*n*) пороговой схемы разделения секрета выбирается полином $p_i(z)$, степень которого превышает полиномиальную форму секрета *M(z)*, т.е.

$$\deg\ p_l(z) > \deg M(z) \quad (7)$$

где *M* – секрет.

Затем выбираются неприводимые полиномы $p_i(z)$, удовлетворяющие условию

$$\deg\ p_i(z) \leq \deg\ p_l(z) \quad (8)$$

где $i = 1,2,...,n$.

При этом степени полиномов должны быть упорядочены по возрастанию

$$\deg\ p_1(z) < \deg\ p_2(z) \leq \deg\ p_3(z) ... \leq \deg\ p_n(z). \quad (9)$$

Для создания (*m*,*n*) –схемы проверяется выполнение условия

$$\deg\ (p_1(z) \cdot p_2(z) \cdot ... p_m(z)) > \deg\ (p_l(z) \cdot p_{n-m+2}(z) \cdot p_{n-m+3}(z) ... p_n(z)).$$

(10)

Чтобы определить доли секрета и распределить их между абонентами группы, выбирается полином *r(z)* и вычисляется значение

$$M^*(z) = M(z) + r(z) \cdot p_l(z). \quad (11)$$

В качестве долей для каждого пользователя выступают остатки

$$M_i^*(z) = M(z) \bmod p_i(z). \quad (12)$$

Используя китайскую теорему об остатках, *m* пользователей способны восстановить значение $M^*(z)$, а затем, зная *r(z)* и $p_l(z)$, определить секрет *M(z)*. При этом группа из абонентов не способна будет получить значение *M(z)*. Для эффективной работы *(m,n)*–схемы разделения секрета в ПСКВ необходимо определить предельное значение полинома *r(z)*, которое позволило бы при меньших временных затратах определить $M^*(z)$, а также выполнить преобразование, обратное (6).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: ТРИУМФ, 2003. – 816 с.

2. http://infcryp.ru/content/razdelenie-klyuchei-skhema-shamira

3. http://chinapads.ru/c/s/shema_asmuta_bluma

4. *Иванов М.А.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / *М.А. Иванов, И.В. Чугунов.* М.: КУДИЗ–ОБРАЗ, 2003. – 240с.

5. *Чипига А.А.* Алгоритм обеспечения информационной скрытности для адаптивныхсредств передачи информации [Текст]/ *И.А. Калмыков, А.А.*

6. *Чипига А.Ф.* //Инфокоммуникационные технологии. – 2007. − № 3. − С. 159 – 162.